Rudvalis群と関連する2-designについて (有限群論と代数的組合せ論)

葛田, 一慶

数理解析研究所講究録
第1593巻 2008年 99-104

Rudvalis群と関連する2-designについて

葛田一慶（Kazumichi Kuzuta）
千葉大学理学研究科
(Graduate School of Science, Chiba University)

1 序文

散在型単純群が作用する強正則グラフにおける最大クリーク（コクリーク）の存在性を利用することで、元のグラフの再構成等に関する結果が、堀口-北詰-中空氏らの研究[4],[5],[6] によって得られてきた。今回もその研究の流れのひとつで、Rudvalis群が作用する強正則グラフの、28個の頂点からなる（最大）クリークから得られるある2-designの構成が本稿の主題である。なおこの研究は北詰正顕教授（千葉大学）との共同研究である。

2 Definitions

2.1 Designs

$X, \mathcal{B}$をそれぞれ有限集合とする。各$x \in X, B \in \mathcal{B}$に対して"関係" xIB が成り立つか成り立たないかが定まっているとき、組$(X, \mathcal{B})$を関係Iに関する結合構造と呼ぶ。xIBであるとき、xとBは結合関係にあるという。またXの元を点、$\mathcal{B}$の元をブロックと呼ぶ。

結合構造$(X, \mathcal{B})$が次の条件を満たすとき、$(X, \mathcal{B})$はt-(v, k, λ) *design*、もしくは*t-design*であるという。

$$\begin{cases} |X| = v \\ \forall B \in \mathcal{B}\,;\ |\{v \in X | vIB\}| = k \\ \forall \{x_1, \ldots, x_t\} \in \binom{X}{t}\,;\ |\{B \in \mathcal{B} | x_i IB, 1 \leq \forall i \leq t\}| = \lambda \end{cases}$$

また、$\{x \in X | xIB\} = \{x \in X | xIB'\}$となるブロック$B, B'$はrepeated blockと呼ばれる。我々が扱う"関係"は包含関係だけであるので、Iのかわりに$\in$を用いることにし、$x \in B$であるときxはBに含まれるということにする。

2.2 Strongly regular graphs

Vを有限集合、$E \subset \binom{V}{2}$とし、組$\Gamma = (V, E)$をグラフとする。$E = \binom{V}{2}$のとき、Γは完全グラフ(*complete graph*)と呼ばれる。特にk個の頂点からなるcomplete subgraphを

k-クリーク (k-*clique*) と呼ぶ。また $x \in V$ に対して $\Gamma(x)$ を、$\Gamma(x) = \{y \in V | \{x, y\} \in E\}$ で定義する。

グラフ $\Gamma = (V, E)$ が以下の条件を満たすとき、Γ をパラメータ (v, a, c, d) の強正則グラフ (*strongly regular graph*) と呼ぶ。

$$\begin{cases} |V| = v \\ \forall x \in V \ ; \ |\Gamma(x)| = a \\ \forall \{x, y\} \in E \ ; \ |\Gamma(x) \cap \Gamma(y)| = c \\ \forall \{x, y\} \in \binom{V}{2} \setminus E \ ; \ |\Gamma(x) \cap \Gamma(y)| = d \end{cases}$$

強正則グラフにおけるクリークのサイズの上限は次で与えられる。

Proposition 2.1. *(Hoffuman)*
$\Gamma = (V, E)$ をパラメータ (v, a, c, d) の強正則グラフとし、その隣接行列の最小固有値を $-m$ とする。Γ が k-*clique* C をもつならば

$$k \leq \frac{a}{m} + 1$$

が成立する。ここで等号成立 $\Longleftrightarrow$ $\forall x \in V \setminus C$ に対して、$|\Gamma(x) \cap C| = \frac{k(a-k+1)}{v-k}$

これよりただちに次が示される。

Corollary 2.1. $\Gamma = (V, E)$ をパラメータ (v, a, c, d) の強正則グラフとし、その隣接行列の最小固有値を $-m$ とする。Γ が k-*clique*($k = \frac{a}{m} + 1$) C をもつならば、$(C, V \setminus C)$ は 2-$(k, \frac{k(a-k+1)}{v-k}, c - k + 2)$ *design* となる。ただしその結合関係は、$p \in C, B \in V \setminus C$ に対して、$p \in B \overset{\text{def}}{\Longleftrightarrow} \{p, B\} \in E$ と定める。

この系 2.1 から得られる design のことを我々は *maximum clique design* と呼んでいる。

2.3 Codes

$\mathbb{F}_q$ を有限体とし、$\mathbb{F}_q^n$ を $\mathbb{F}_q$ 上の n 次元ベクトル空間とする。また $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$ に対して、その距離 $d(x, y)$ を $d(x, y) = |\{i | x_i \neq y_i\}|$ と定義する。以下の条件を満たすとき、C を $(n, M, d; q)$ *code* と呼ぶ。

$$\begin{cases} C \subset \mathbb{F}_q^n (\text{subset}) \\ |C| = M \\ \min\{d(x, y) | x, y (\neq) \in C\} = d \end{cases}$$

また、C の任意の異なる 2 つのベクトルの距離が等しいとき、C は等距離符号 (*equidistant code*) であると言われる。

Proposition 2.2. *(Tonchev[8])*
equidistant $(n, M, d; q)$ *code* に対して、次の不等式が成立する。

$$d \le \frac{nM(q-1)}{(M-1)q}$$

この命題において等号が成立する equidistant code を *optimal code* と呼ぶ。

Example 2.1. 次は *optimal* $(7, 8, 6; 4)$ *code* である。この符号を C_1 と書くことにする。

$$\begin{array}{c}
(\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ )\\
(\ 0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 1\ \ 1\ )\\
(\ 1\ \ 0\ \ 1\ \ \omega\ \ \omega\ \ \omega\ \ \omega\ )\\
(\ 1\ \ 1\ \ 0\ \ \omega^2\ \ \omega^2\ \ \omega^2\ \ \omega^2\ )\\
(\ \omega\ \ \omega\ \ \omega\ \ 0\ \ 1\ \ \omega\ \ \omega^2\ )\\
(\ \omega\ \ \omega^2\ \ \omega^2\ \ 1\ \ 0\ \ \omega^2\ \ \omega\ )\\
(\ \omega^2\ \ \omega\ \ \omega^2\ \ \omega\ \ \omega^2\ \ 0\ \ 1\ )\\
(\ \omega^2\ \ \omega^2\ \ \omega\ \ \omega^2\ \ \omega\ \ 1\ \ 0\ )
\end{array}$$

この符号 C_1 は和について閉じている、すなわち $\mathbb{F}_4^7$ における加法群になっていることに注意したい。

3 Rudvalis-graph

Ru を Rudvalis 群とする。28 次元複素ベクトル空間において、その自己同型群が 4.Ru となるある格子が存在する。この格子にはノルムが 4 のベクトルが 4×4060 個存在しており、これらがその格子を生成している。このノルム 4 のベクトルは *sacred vector* と呼ばれている。

今、頂点を $(\pm 1, \pm i$ 倍を無視した)4060 個のノルム 4 ベクトルと考え、2 つのベクトルが直交するときに限り 2 頂点が隣接することにすると、パラメータ $(4060, 1755, 730, 780)$ の強正則グラフが出来る。このグラフを Rudvalis-graph と呼び、Γ_{Ru} と書くことにする。$\mathrm{Aut}(\Gamma_{\mathrm{Ru}}) \cong \mathrm{Ru}$ である。

Γ_{Ru} の場合、命題 2.1 における上限は 28 になるが、実際に 28-clique がグラフの自己同型の作用を除いて一意的に存在することが分かった。したがって系 2.1 より、そこから maximum clique 2-$(28, 12, 704)$ design ができるが、詳しく調べてみるとこの design は、16-repeated 2-$(28, 12, 44)$ design となっている。この 2-$(28, 12, 44)$ design のことを D_{Ru} と書くことにする。D_{Ru} は、simple な (repeat のない) ブロックと 4-repeated になっているブロックの 2 種類のブロックを持っていることに注意しておく。

4 D_{Ru} の構成

Γ_{Ru} から得られた D_{Ru} の構造を明らかにすることがここでの目標である。まず 28 点集合 X を次のように 4×7 の配列として考える。

$X =$

1	2	3	4	5	6	7

次に例 2.1 であげた符号 $\mathcal{C}_1$ の（all-0 word を除く）各 codeword から次の、codeword の成分と X の列の対応規則と、条件:「第 1 行における parity は odd」 を満たす X の 12-部分集合を全て考える。

$$0 \rightarrow \phi = \begin{bmatrix} \\ \\ \\ \\ \end{bmatrix}, 1 \rightarrow \begin{bmatrix} \circ \\ \circ \\ \\ \\ \end{bmatrix}, \begin{bmatrix} \\ \\ \circ \\ \circ \end{bmatrix}, \omega \rightarrow \begin{bmatrix} \circ \\ \\ \circ \\ \\ \end{bmatrix}, \begin{bmatrix} \\ \circ \\ \\ \circ \end{bmatrix}, \omega^2 \rightarrow \begin{bmatrix} \circ \\ \\ \\ \circ \end{bmatrix}, \begin{bmatrix} \\ \circ \\ \circ \\ \\ \end{bmatrix}$$

Example 4.1. 例えば次のような 12-部分集合は (0111111) から構成される。

		○		○		○
		○		○		○
	○		○		○	
	○		○		○	

				○		
				○		
	○	○	○		○	○
	○	○	○		○	○

このようにして構成される X の 12-部分集合全体からなる族を $\mathcal{B}_1$ とする。

次に 7 点集合 P とその 3-部分集合族 L を次のように定める。

$$\begin{aligned} P &= \{1, \ldots, 7\} \\ L &= \{\{1,2,3\}, \{1,4,5\}, \{1,6,7\}, \{2,4,6\}, \{2,5,7\}, \{3,4,7\}, \{3,5,6\}\} \end{aligned}$$

(P, L) は 2-(7, 3, 1) design(位数 2 の射影平面) である。L のブロック $B = \{i, j, k\}$ に対して X の i, j, k 列の全ての点からなる 12 点を対応させることにする。

Example 4.2. 例えばブロック $\{1, 4, 5\}$ からは次のような 12-部分集合が対応する。

○			○	○		
○			○	○		
○			○	○		
○			○	○		

ここではさらに、この方法で得られた各々の X の 12-部分集合を 4 回ずつ繰り返させてできる族を考え、これを $\mathcal{B}_2$ とおくことにする。

以上のように、code $\mathcal{C}_1$ とブロック集合 L からできる結合構造 $(X, \mathcal{B}_1 \cup \mathcal{B}_2)$ を $D(\mathcal{C}_1, L)$ と書くことにする。このとき次が成り立つ。

Theorem 4.1. $D(C_1, L)$ は D_{Ru} と同型である。

同型判定は計算機 (Magma) による。一般に、all-0 word を含む optimal $(7, 8, 6, 4)$ code $\mathcal{C}$ と、2-$(7, 3, 1)$ design のブロック集合 $\mathcal{B}$ に対して、$D(\mathcal{C}, \mathcal{B})$ は 2-$(28, 12, 44)$ design になるが、これが D_{Ru} と同型になるとは限らない。2-$(7, 3, 1)$ design の design としての構造は一意的であるが、ブロック集合 L を具体的に記述したのはこのことが理由である。実際は次が言える。

Theorem 4.2. *optimal additive* $(7, 8, 6, 4)$ *code* $\mathcal{C}$ は同値を除いて一意的に存在する。さらにこのとき $D(\mathcal{C}, \mathcal{B})$ が D_{Ru} と同型になるような 2-$(7, 3, 1)$ *design* のブロック集合 $\mathcal{B}$ が一意的に存在する。

ここで additive というのは和について閉じていることを意味し、座標の置換と各成分ごとの $\{1, \omega, \omega^2\}$ の置換をして得られる符号を同値な符号として考えている。

最後に D_{Ru} と sacred vector の関係について述べる。3 節で述べたように、その自己同型群が 4.Ru になる、sacred vector によって生成される 28 次元複素ベクトル空間におけるある格子が存在する。Conway[1] によれば orthonormal frame をなす 28 個のベクトル $e_i (i = 1, \ldots, 28)$ で、$4e_i$ が sacred vector になるものが存在する。この frame を使って格子のベクトルを表示すると、($4e_i$ は除けば) その成分が 0 となる座標が 12 個、0 以外 $(\pm 1, \pm i)$ となる座標が 16 個存在している。この成分が 0 になる 12 個の座標と D_{Ru} のブロックが対応しているのである。したがって当然、sacred vector と D_{Ru} の関係を明らかにしたいわけであるが、Γ_{Ru} から得られた maximum clique design が 16-repeated D_{Ru} となっていたことに対応して、D_{Ru} の 1 つのブロックには 16 個の sacred vector が対応している。そのため現在は、D_{Ru} だけを用いて sacred vector 全体を (シンプルに) 記述することは難しいと考えている。しかしこの記述ができるような数学的背景がこれらの間にあれば面白いと思われる。

参考文献

[1] J. H. Conway, A quaternionic construction for the Rudvalis Group, In Topics in group theory and computation (Proc. Summer School, University Coll., Galway, 1973), 69-81, Academic Press, London, 1977.

[2] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, ATLAS of finite groups, Oxford University Press, Eynsham, 1985.

[3] J. H. Conway and D. B. Wales, Construction of the Rudvalis group of order 145 926 144 000, J. Algebra 27 (1973), 538-548.

[4] N. Horiguchi, M. Kitazume and H. Nakasora, The Hall-Janko graph and the Witt system W_{10}, European J. Combin. 29 (2008), 1-8.

[5] N. Horiguchi, M. Kitazume and H. Nakasora, A construction of the sporadic Suzuki graph from $U_3(4)$, preprint.

[6] N. Horiguchi, M. Kitazume and H. Nakasora, On the maximum coclique of the rank 3 graph of $2^{11}.M_{24}$, preprint.

[7] X. L. Hubaut, Strongly regular graphs, Discrete Math. 13 (1975), 357-381.

[8] V. D. Tonchev, Combinatorial Configurations Designs, Codes, Graphs, Pitman Monographs and Surveys in Pure and Applied Mathematics, Vol40. Longman, New York, 1988 (Translated from Bulgarian by Robert A. Melter).